ESET MOBILE SECURITY

POUR ANDROID

Manuel d'installation et Guide de l'utilisateur

Veuillez cliquer ici pour obtenir la version la plus récente de ce document.

Contenu

1. Installation d'ESET Mobile Security.....3
1.1 Installation.....3
1.2 Désinstallation.....3
2. Activation de produit.....4
3. Antivirus.....4
4. Antipourriel.....7
5. Anti-vol.....8
6. Audit de sécurité.....9
7. Mise à jour.....10
8. Mot de passe.....10
9. Dépannage et assistance.....11
9.1 Dépannage.....11
9.2 Assistance technique.....11

ESET **MOBILE SECURITY**

©2012 ESET, spol. s r.o.
ESET Mobile Security a été développé par ESET, spol. s r.o.
Pour plus d'information, visitez www.eset.com.
Tous droits réservés. Aucune partie de cette documentation ne peut être reproduite, stockée dans un système d'archivage ou transmise sous quelque forme ou par quelque moyen que ce soit, y compris sous forme électronique, mécanique, photocopie, enregistrement, numérisation ou autre sans l'autorisation écrite de l'auteur.
ESET, spol. s r.o. se réserve le droit de changer les applications décrites sans préavis.

Assistance à la clientèle : www.eset.com/support

RÉV. 25. 4. 2012

1. Installation d'ESET Mobile Security

Pour installer ESET Mobile Security pour Android, la configuration minimale requise de votre périphérique mobile est la suivante :

	Configuration minimale requise
Système d'exploitation	Android 2.0/2.1 (Éclair) et versions ultérieures
CPU	600 MHz
RAM	256 Mo
Espace libre sur le stockage interne	5 Mo

REMARQUE : certaines fonctionnalités (l'antipourriel et Anti-Theft, par exemple) ne sont pas disponibles sur Android 3.0 ou sur les tablettes qui ne prennent pas les appels et la messagerie en charge. Vous trouverez plus de détails dans cet article de la base de connaissances (peut ne pas être disponible dans votre langue).

1.1 Installation

Pour installer ESET Mobile Security, effectuez l'une des opérations suivantes :

- trouvez ESET Mobile Security (ou seulement Eset) dans l'application Google Play Store sur votre périphérique Android. ESET Mobile Security se trouve dans **Applications** > **Outils**. Vous pouvez également installer le programme en saisissant le code QR ci-dessous à l'aide de votre périphérique mobile et d'une application comme QR Droid ou Barcode Scanner.

- téléchargez le fichier d'installation d'ESET Mobile Security *(ems.apk)* à partir du site Web d'ESET en saisissant le code QR ci-dessous.

- téléchargez le fichier *ems.apk* sur votre ordinateur à partir du site Web d'ESET. Copiez le fichier sur votre périphérique par Bluetooth ou USB. Appuyez sur l'icône de lancement de l'écran d'accueil Android (ou rendez-vous sur **Accueil** > **Menu**) et appuyez sur **Paramètres** > **Applications** et assurez-vous que l'option **Sources inconnues** est sélectionnée. Trouvez le fichier *ems.apk* à l'aide d'une application comme ASTRO File Manager ou ES File Explorer. Ouvrez le fichier et appuyez sur **Installer**. Une fois l'application installée, appuyez sur **Ouvrir.**

Avertissement : ESET Mobile Security doit être installé sur le stockage interne du périphérique. Certains téléphones mobiles autorisent par erreur les utilisateurs à installer des applications sur la carte SD. Si vous installez ESET Mobile Security sur la carte SD, les fonctions Protection en temps réel, Antipourriel et Anti-vol ne fonctionneront pas.

Une fois l'installation réussie, activez ESET Mobile Security en suivant les étapes de la section Activation de produit 4.

1.2 Désinstallation

Si vous souhaitez désinstaller ESET Mobile Security de votre périphérique, utilisez l'**assistant de désinstallation**, accessible à partir de l'écran principal d'ESET Mobile Security ou suivez les étapes indiquées ci-dessous :

1. Appuyez sur l'icône de lancement sur l'écran d'accueil Android (ou ouvrez **Accueil** > **Menu**) et appuyez sur **Paramètres** > **Localisation et sécurité** > **Administrateurs du mobile**, désélectionnez **ESET Security** et appuyez sur **Désactiver**. Entrez votre mot de passe ESET Mobile Security quand on vous le demandera. (Si vous n'avez pas défini ESET Mobile Security en tant qu'administrateur du mobile, ignorez cette étape.)
2. Retournez aux **Paramètres** et appuyez sur **Applications** > **Gérer les applications** > **ESET Security** > **Désinstaller**.

ESET Mobile Security et le dossier de quarantaine seront supprimés de façon permanente de votre périphérique mobile.

2. Activation de produit

Une fois l'installation réussie, ESET Mobile Security doit être activé. Appuyez sur **Activer maintenant**, sur l'écran principal d'ESET Mobile Security.

Les méthodes d'activation varient selon que vous avez téléchargé ESET Mobile Security à partir du site Web d'ESET ou de Google Play.

- **Activer l'essai** - sélectionnez cette option si vous ne possédez pas de licence et que vous souhaitez faire l'essai d'ESET Mobile Security avant d'en faire l'achat. Inscrivez votre **adresse courriel** afin d'activer ESET Mobile Security pour une durée limitée. Vous recevrez un courriel de confirmation une fois l'activation terminée. Les licences d'essai ne peuvent être activées qu'une seule fois par périphérique mobile.
- **Activer à l'aide d'une clé d'activation** - (cette option n'est pas disponible si vous avez installé ESET Mobile Security à partir de Google Play) si vous avez acquis le programme avec un nouveau périphérique (ou avez acheté une version commerciale du produit), vous avez reçu une clé d'activation avec votre achat. Entrez l'information que vous avez reçue dans le champ **Clé d'activation** et votre adresse courriel actuelle dans le champ **Courriel**. Vos nouvelles données d'authentification (nom d'utilisateur et mot de passe) remplaceront automatiquement la clé d'activation et seront envoyées à l'adresse courriel que vous avez spécifiée.
- **Activer à l'aide d'un nom d'utilisateur et d'un mot de passe** - (cette option n'est pas disponible si vous avez installé ESET Mobile Security à partir de Google Play) si vous avez acheté votre produit auprès d'un distributeur, vous avez reçu un nom d'utilisateur et un mot de passe avec votre achat. Entrez les informations que vous avez reçues dans les champs **Nom d'utilisateur** et **Mot de passe**. Entrez votre adresse courriel actuelle dans le champ **Courriel**.
- **Renouveler la licence** - sélectionnez cette option si votre licence actuelle expirera bientôt. Entrez votre **Nom d'utilisateur** et votre **Mot de passe** (données fournies au moment de l'achat de la licence actuelle) dans les champs appropriés.
- **Charger les données de licence** - (cette option n'est pas disponible si vous avez téléchargé ESET Mobile Security à partir du site Web d'ESET) utilisez cette option si vous avez déjà acheté le programme avec compte. ESET Mobile Security sera activé en chargeant vos données de licence à partir du serveur ESET.
- **Acheter maintenant** - sélectionnez cette option si vous ne possédez pas de licence et que vous souhaitez en acheter une.

Chaque activation est valide pour une période de temps limitée. Une fois l'activation expirée, vous serez invité à renouveler la licence du programme (le programme vous avertira à l'avance).

REMARQUE : Lors de l'activation, le périphérique doit être connecté à Internet. Cela nécessite le téléchargement d'une petite quantité de données.

Par défaut, ESET Mobile Security est installé dans la langue qui est définie sur votre téléphone comme paramètres régionaux (dans les paramètres de langue et de clavier). Si vous souhaitez changer la langue de toute l'interface utilisateur de l'application, appuyez sur **Langue** dans l'écran principal ESET Mobile Security et sélectionnez la langue de votre choix.

3. Antivirus

Analyser le mobile

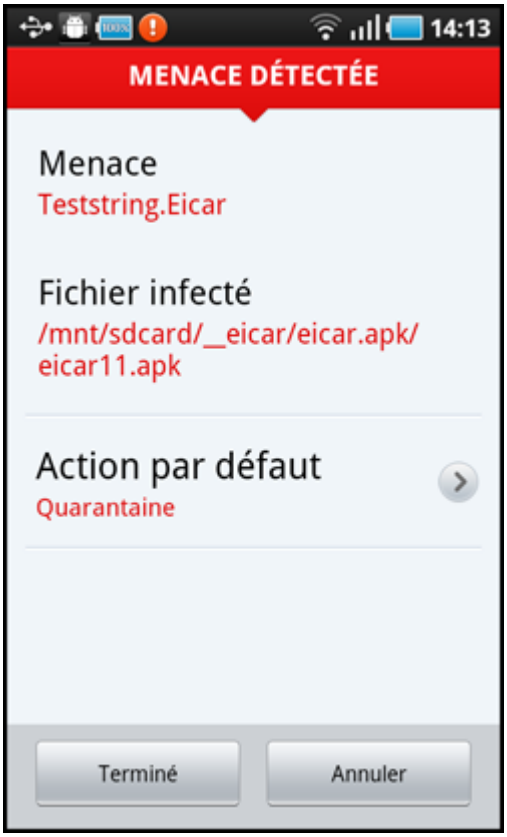
L'option **Analyser le mobile** peut être utilisée pour rechercher des infiltrations.

Certains types de fichiers prédéfinis sont analysés par défaut. L'analyse complète du mobile vérifie la mémoire, les processus en cours, leurs bibliothèques de liens dynamiques et les fichiers qui font partie du stockage interne et amovible. Un bref résumé de l'analyse s'affiche une fois l'analyse terminée (indiquant le nombre de fichiers infectés, le nombre de fichiers analysés, la durée de l'analyse, etc.).

Si vous souhaitez abandonner une analyse en cours, appuyez sur **Annuler**.

Analyser le répertoire

Pour analyser des répertoires en particulier, appuyez sur **Analyser le répertoire**. Trouvez les dossiers que vous souhaitez analyser, appuyez sur les cases à cocher dans la colonne de droite et appuyez sur **Analyser**.



Menace détectée par ESET Mobile Security

Journaux d'analyse

La section **Journaux d'analyse** contient des journaux fournissant les données complètes au sujet des tâches d'analyse terminées. Les journaux sont créés après chaque analyse déclenchée manuellement (à la demande) ou lorsqu'une infiltration est détectée par une analyse en temps réel.

Chaque journal contient :

- la date et l'heure de l'événement,
- le nombre de fichiers analysés,
- le nombre de fichiers infectés,
- le chemin d'accès complet des fichiers infectés,
- la durée de l'analyse,
- les actions exécutées ou les erreurs rencontrées lors de l'analyse.

Quarantaine

La principale fonction de la quarantaine est le stockage en toute sécurité des fichiers infectés. Ces fichiers doivent être mis en quarantaine s'ils ne peuvent pas être nettoyés, s'il est risqué ou déconseillé de les supprimer ou s'ils sont détectés par erreur par ESET Mobile Security.

Les fichiers stockés dans la quarantaine sont indiqués dans un journal qui affiche le nom et l'emplacement d'origine du fichier infecté ainsi que la date et l'heure de mise en quarantaine.

Si vous souhaitez restaurer un fichier en quarantaine vers son emplacement d'origine, appuyez sur le fichier et sélectionnez **Restaurer**. Il n'est pas recommandé de choisir cette option.

Pour retirer un fichier en quarantaine de façon permanente à partir de votre périphérique, appuyez sur le fichier, puis sélectionnez **Supprimer**. Pour retirer tous les fichiers stockés dans la quarantaine, appuyez sur le bouton **MENU**, suivi de **Supprimer tout**.

Paramètres

Les paramètres **À la demande** vous permettent de modifier les paramètres de l'analyse déclenchée manuellement (à la demande).

L'option **Afficher les alertes** affiche les notifications de menace à mesure qu'une nouvelle menace est détectée par l'analyseur à la demande.

Si vous souhaitez analyser toutes les applications (fichiers *.apk*) installées sur votre périphérique, sélectionnez l'option **Analyser les applications**.

La **Protection proactive** est une méthode de détection basée sur un algorithme qui analyse le code et recherche le comportement typique d'un virus. Son principal avantage est sa capacité à identifier les programmes malveillants qui n'ont pas encore été reconnus par la base de données de virus. L'analyse nécessitera plus de temps si la protection proactive est activée.

L'option **Profondeur d'analyse des archives** vous permet de spécifier la profondeur d'imbrication des archives (fichiers *.zip*) à analyser. Plus le nombre est élevé, plus l'analyse se fera en profondeur.

L'option **Stockage des journaux** vous permet de définir le nombre maximal de journaux qui peuvent être stockés dans la section **Journaux d'analyse** 5.

Vous pouvez spécifier une **action par défaut** qui sera effectuée automatiquement lors de la détection de fichiers infectés. Vous pouvez choisir parmi les options suivantes :

- **Ignorer** - aucune mesure ne sera prise concernant le fichier infecté (cette option n'est pas recommandée),
- **Supprimer** - le fichier infecté sera supprimé,
- **Quarantaine** - (par défaut) le fichier infecté sera placé en **Quarantaine** 5.

Les paramètres **Extensions** affichent les types de fichier les plus courants exposés aux infiltrations sur la plateforme Android. Sélectionnez le type de fichier que vous souhaitez analyser ou désélectionnez les extensions que vous souhaitez exclure de l'analyse. Ces paramètres s'appliquent à l'analyse à la demande et à l'analyse en temps réel :

- **Sensible aux extensions** - si vous désactivez cette option, tous les types de fichiers seront analysés. Les fichiers seront également analysés s'ils n'ont pas été déguisés en un autre type de fichier. En conséquence, l'analyse sera plus longue.
- **DEX (fichier du code applicatif)** - format de fichier exécutable qui contient le code compilé écrit pour le système d'exploitation Android,
- **SO (bibliothèques)** - bibliothèques partagées sauvegardées dans un endroit désigné du système de fichiers et reliées par des programmes qui requièrent leurs fonctions,
- **Archives (fichiers compressés)** - fichiers compressés à l'aide de la compression Zip,
- **Autres** - autres types de fichiers connus.

Dans les paramètres **En temps réel**, vous pouvez configurer les paramètres de l'analyseur à l'accès. L'analyseur à l'accès analyse les fichiers que vous utilisez en temps réel. Elle analyse automatiquement le dossier *Téléchargement* de la carte SD, les fichiers d'installation *.apk* et les fichiers de la carte SD montée (si l'option **Analyser les cartes SD montées** est activée). L'analyseur à l'accès est lancée automatiquement lors du démarrage du système.

- **Protection en temps réel** - si elle est activée (par défaut), l'analyseur à l'accès s'exécute en arrière-plan.
- **Afficher les alertes** - affiche les notifications de menace à mesure qu'une nouvelle menace est détectée par l'analyseur à l'accès.
- **Analyser les cartes SD montées** - analyse les fichiers avant de les ouvrir ou de les sauvegarder sur la carte SD.
- **Protection proactive** - sélectionnez cette option pour appliquer des techniques d'analyse heuristiques. L'heuristique identifie les nouveaux logiciels malveillants qui ne sont pas encore reconnus par la base de données de virus de façon proactive, en analysant le code et en reconnaissant le comportement typique d'un virus. L'analyse nécessite plus de temps si la protection proactive est activée.
- **Profondeur d'analyse des archives** - cette option vous permet de spécifier la profondeur d'imbrication des archives (fichiers *.zip*) à analyser. Plus le nombre est élevé, plus l'analyse se fera en profondeur.

- **Action par défaut** - vous pouvez spécifier une action par défaut qui sera effectuée automatiquement lorsque l'analyseur à l'accès détecte des fichiers infectés. Si vous sélectionnez **Ignorer**, aucune mesure ne sera prise concernant le fichier infecté (cette option n'est pas recommandée). Si vous sélectionnez **Supprimer,** le fichier infecté sera supprimé. Si vous sélectionnez **Quarantaine**, le fichier infecté sera placé en **Quarantaine** 5.

ESET Mobile Security affiche une icône dans le coin supérieur gauche de l'écran (barre d'état Android). Si vous ne voulez pas que cette icône soit affichée, allez à l'écran principal d'ESET Mobile Security, appuyez sur **MENU**, suivi de **Notifications** et désélectionnez l'option **Afficher l'icône**. Veuillez noter que cela ne désactive pas l'icône d'avertissement rouge avec un point d'exclamation qui vous informe d'un risque de sécurité (par exemple, l'analyse virale en temps réel désactivée, la correspondance de carte SIM désactivée, etc.).

4. Antipourriel

Le module **Antipourriel** bloque les messages SMS/MMS entrants et les appels entrants et sortants en fonction des règles que vous avez définies.

Les messages non sollicités incluent généralement des publicités provenant de fournisseurs de services de téléphonie cellulaire ou des messages d'utilisateurs inconnus ou non spécifiés. Le terme *bloquer les contacts* désigne le transfert automatique des messages entrants vers la section **Journaux des pourriels** 7. Vous ne recevez aucune notification lorsque le message entrant est bloqué. L'avantage est que vous ne serez pas dérangé par des informations non sollicitées, mais vous pouvez toujours vérifier les journaux au cas où des messages auraient été bloqués par erreur.

Pour ajouter une nouvelle règle antipourriel, appuyez sur **Liste des règles SMS et Appels** > **Ajouter nouvelle**. Entrez le numéro de téléphone que vous souhaitez bloquer ou appuyez sur **+** pour choisir le numéro à partir de votre liste de contacts. Personnalisez la règle en autorisant ou en bloquant les messages et les appels et appuyez sur **Terminé**.

Pour modifier ou retirer une règle existante, appuyez sur l'entrée et maintenez appuyée, puis choisissez l'action voulue. Si vous souhaitez supprimer toutes les règles, appuyez sur **MENU**, suivi de **Tout retirer**.

REMARQUE : Le numéro de téléphone doit inclure l'indicatif international suivi du numéro (p. ex. +16101001OO).

Liste des règles Antispam

Paramètres

Bloquer les appels anonymes - activez cette option si vous souhaitez bloquer les appelants dont le numéro de téléphone est intentionnellement masqué par le refus d'identification de la ligne appelante (CLIR).

Bloquer les contacts connus - utilisez cette option pour bloquer les messages et les appels de personnes qui figurent parmi votre liste de contacts.

Bloquer les contacts inconnus - utilisez cette option pour bloquer les messages et les appels de personnes qui ne figurent pas parmi votre liste de contacts. Vous pouvez utiliser cette option pour bloquer les appels indésirables (p. ex. les appels de sollicitation à froid) ou empêcher les enfants de composer des numéros inconnus. (Pour éviter cela, il est recommandé de protéger vos paramètres antipourriel avec un **mot de passe** 10.)

Dans la section **Journaux des pourriels**, vous pouvez voir les appels et les messages qui ont été bloqués par le module antipourriel. Chaque journal contient le nom de l'événement, le numéro de téléphone correspondant ainsi que la date et l'heure de l'événement. Les messages SMS bloqués contiennent également le corps du message.

5. Anti-vol

La fonctionnalité **Anti-vol** protège votre téléphone cellulaire contre les accès non autorisés.

Si vous perdez votre téléphone ou que quelqu'un le vole et remplace votre carte SIM par une nouvelle carte (non sécurisée), ESET Mobile Security verrouillera automatiquement votre téléphone. Une alerte SMS sera envoyée secrètement au(x) numéro(s) de téléphone défini(s) par l'utilisateur. Ce message contiendra le numéro de téléphone de la carte SIM qui est insérée, l'IMSI (identification internationale d'abonné mobile) et l'IMEI (identité internationale d'équipement mobile) du téléphone. L'utilisateur non autorisé ne saura pas que ce message a été envoyé puisqu'il sera automatiquement supprimé du fil de **Messagerie**. De plus, vous pouvez également demander les coordonnées GPS de votre téléphone cellulaire perdu ou effacer les données stockées sur le mobile à distance.

Cartes SIM de confiance

Si la carte SIM actuellement dans votre téléphone cellulaire est celle que vous souhaitez enregistrer en tant que carte de confiance, appuyez sur **Ajouter**. Si vous utilisez plus d'une carte SIM, vous voudrez peut-être distinguer chacune d'elle en modifiant l'**Alias de la carte SIM** (par exemple, *bureau*, *maison*, etc.).

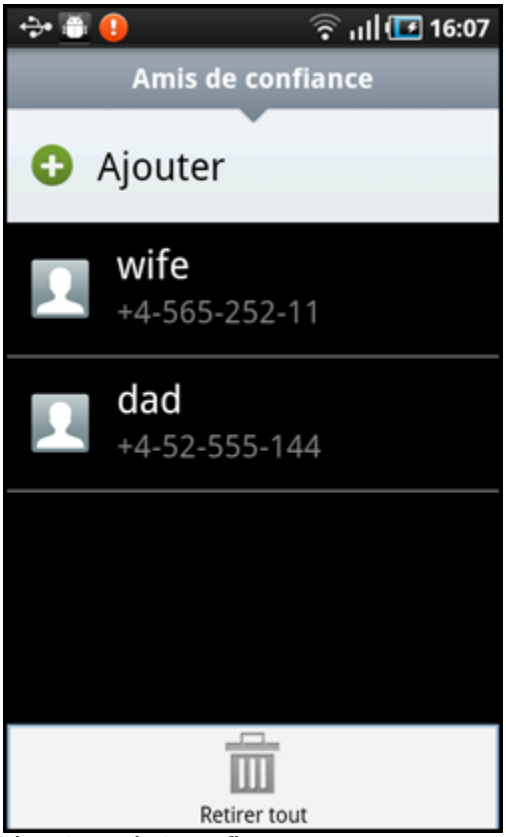
Pour **modifier** ou **retirer** l'entrée d'une carte SIM, appuyez sur l'entrée et maintenez appuyée, puis choisissez l'action voulue. Si vous souhaitez retirer toutes les entrées de la liste, appuyez sur **MENU**, suivi de **Tout retirer**.

Amis de confiance

Dans la liste des **amis de confiance,** appuyez sur **Ajouter** pour ajouter les numéros de téléphone qui recevront une alerte SMS si une carte SIM non sécurisée est insérée dans votre mobile. Entrez un nom dans le champ **Nom de l'ami** et son numéro de téléphone dans le champ **Numéro de téléphone** ou appuyez sur le bouton **+** pour choisir un contact parmi votre liste de contacts. Si le contact possède plus d'un numéro de téléphone, l'alerte SMS sera envoyée à tous les numéros.

Pour **modifier** ou **retirer** une entrée existante, appuyez sur l'entrée et maintenez appuyée, puis choisissez l'action voulue. Si vous souhaitez retirer toutes les entrées de la liste, appuyez sur **MENU**, suivi de **Tout retirer**.

REMARQUE : Le numéro de téléphone doit inclure l'indicatif international suivi du numéro (p. ex. +16101001OO).



Liste des amis de confiance

Paramètres

Si vous possédez un périphérique sans carte SIM (p. ex. une tablette ou un téléphone AMRC), sélectionnez l'option **Ignorer la correspondance SIM**. Cela désactivera les avertissements rouges *Risque de sécurité!* (*correspondance de carte SIM désactivée* et *Aucune carte SIM de confiance définie*) à partir de l'écran principal d'ESET Mobile Security. (Veuillez noter que l'option Ignorer la correspondance SIM est grisée sur les périphériques AMRC.)

Pour activer la vérification automatique de la carte SIM insérée (et l'envoi de l'alerte SMS), sélectionnez l'option **Activer la correspondance SIM**.

Dans le champ **Texte de l'alerte SMS**, vous pouvez modifier le texte du message qui sera envoyé au(x) numéro(s) de téléphone prédéfini(s) si une carte SIM non sécurisée est insérée dans votre mobile. Si vous avez acheté ESET Mobile Security sur Google Play, une adresse courriel de votre compte Google est insérée automatiquement. Vous pouvez également entrer une autre adresse courriel ou un autre numéro de contact.

Commandes SMS

Les commandes SMS à distance (effacer, verrouiller et trouver) ne fonctionneront que si l'option **Activer les commandes par SMS** est sélectionnée.

L'option **Activer la réinitialisation du mot de passe par SMS** vous permet de réinitialiser votre mot de passe de sécurité en envoyant un SMS depuis un

numéro de téléphone sauvegardé dans votre liste d' **amis de confiance** vers votre numéro de téléphone. Le SMS doit respecter le format suivant :
eset remote reset

Si vous perdez votre téléphone et que vous souhaitez le verrouiller, envoyez un SMS de verrouillage à distance depuis n'importe quel mobile vers votre numéro de téléphone en respectant le format suivant :
eset lock mot de passe
Remplacez *mot de passe* par votre propre mot de passe défini dans la section **Mot de passe** 10. Un utilisateur non autorisé ne pourra pas utiliser votre téléphone puisqu'il aura besoin de votre mot de passe.

Si vous souhaitez demander les coordonnées GPS de votre mobile, envoyez une commande SMS à votre numéro de téléphone ou au numéro de téléphone de l'utilisateur non autorisé (si la carte SIM a déjà été remplacée) :
eset find mot de passe
Vous recevrez un SMS avec les coordonnées GPS et un lien vers Google Maps, vous indiquant l'emplacement exact de votre mobile. Veuillez noter que pour recevoir les coordonnées GPS, le module GPS de votre téléphone doit être activé à l'avance.

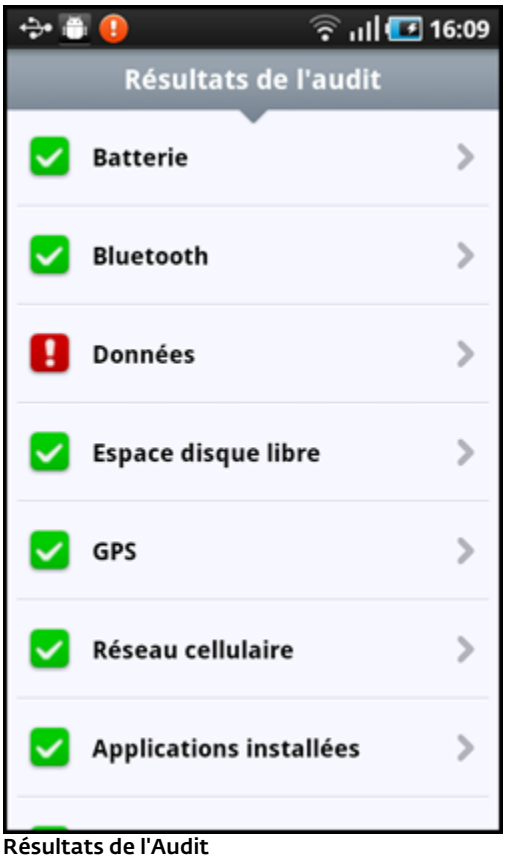
Si vous souhaitez effacer toutes les données stockées sur votre mobile et sur tout support amovible inséré, envoyez une commande SMS d'effacement à distance :
eset wipe mot de passe
Tous les contacts, les messages, les courriels, les applications installées, votre compte Google et le contenu de la carte SD seront effacés de façon permanente de votre mobile. Si ESET Mobile Security n'est pas défini en tant qu'administrateur du mobile, seuls les contacts, les messages et le contenu de la carte SD seront effacés.

REMARQUE : Le mot de passe est sensible à la casse. Veuillez vous assurer d'entrer votre mot de passe de la même façon que vous l'avez défini dans la section Mot de passe.

6. Audit de sécurité

L'audit de sécurité vérifie l'état du téléphone y compris le niveau de batterie, l'état Bluetooth et l'espace disque libre.

Pour exécuter un audit de sécurité manuellement, appuyez sur **Audit**. Un rapport détaillé sera affiché.



Résultats de l'Audit

Un crochet vert à côté de chaque élément indique que la valeur est supérieure à la limite ou que l'élément ne représente pas un risque de sécurité.

Une icône jaune signifie qu'au moins l'un des éléments est inférieur à la limite ou que l'élément peut représenter un risque de sécurité potentiel. Appuyez sur l'élément pour voir les résultats détaillés.

Un point d'exclamation rouge indique que l'élément est inférieur à la limite ou que l'élément représente un risque de sécurité et doit être corrigé.

Si vous souhaitez corriger l'état de l'élément en surbrillance de couleur rouge, appuyez sur l'élément et confirmez en appuyant sur **Oui**.

Paramètres

Par défaut, l'audit de sécurité s'exécute périodiquement toutes les 24 heures. Si vous souhaitez désactiver l'audit périodique, désélectionnez l'option **Faire un audit régulièrement**.

Si l'option **Corriger automatiquement** est activée, ESET Mobile Security tentera automatiquement de corriger les éléments à risque (état bluetooth, par ex.) sans intervention de la part de l'utilisateur. Cette option s'applique uniquement à l'audit périodique (planifié).

L'option **Stockage des journaux** vous permet de définir le nombre maximal de journaux qui peuvent être stockés dans la section **Journaux d'audit**.

L'option **Période d'audit** vous permet de définir à quelle fréquence l'audit périodique (planifié) sera exécuté.

Pour ajuster la valeur limite à laquelle l'espace disque libre et le niveau de batterie seront considérés comme étant insuffisants, utilisez les options **Limite d'espace libre du disque** et **Limite du niveau de batterie**.

Sous l'onglet **Éléments de l'audit**, sélectionnez les éléments à vérifier lors de l'audit périodique (planifié).

La section **Journaux d'audit** contient des journaux fournissant les données complètes au sujet des audits périodiques et des audits déclenchés manuellement qui ont eu lieu. Chaque journal contient la date et l'heure de l'événement ainsi que les résultats détaillés de chaque élément.

Le **Gestionnaire de tâches** ournit un aperçu de tous les processus, services et tâches en cours d'exécution sur votre périphérique. ESET Mobile Security vous permet de mettre fin aux processus, services et tâches non exécutés par le système. Ces derniers sont identifiables par une icône rouge (**x**).

7. Mise à jour

Par défaut, ESET Mobile Security est installé avec une tâche de mise à jour pour s'assurer que le programme est mis à jour régulièrement. Pour exécuter la mise à jour manuellement, appuyez sur **Mise à jour maintenant**.

Paramètres

L'option **Mise à jour automatique** vous permet de définir un intervalle de temps pour effectuer le téléchargement automatique des mises à jour de la base de données de virus.

REMARQUE : Pour éviter toute utilisation inutile de bande passante, les mises à jour sont publiées au fur et à mesure des besoins, lorsqu'une nouvelle menace est détectée. Bien que les mises à jour soient gratuites avec votre licence active, votre fournisseur de services sans fil pourrait vous facturer pour les transferts de données.

8. Mot de passe

Votre mot de passe de sécurité protège vos paramètres contre des modifications non autorisées. Le mot de passe est nécessaire pour :

- accéder à des fonctionnalités d'ESET Mobile Security qui sont protégées par un mot de passe (antivirus, antipourriel, anti-vol et audit de sécurité),
- accéder à votre téléphone s'il est verrouillé,
- envoyer des commandes SMS à votre périphérique,
- désinstaller ESET Mobile Security.

REMARQUE : La protection pour la désinstallation n'est disponible que pour Android 2.2 et versions ultérieures.

Pour définir un nouveau mot de passe de sécurité, écrivez-le dans les champs **Mot de passe** et **Entrer à nouveau le mot de passe**. L'option **Phrase de rappel** (si définie) affiche un indice si vous avez oublié votre mot de passe.

IMPORTANT : Veuillez prendre le temps de bien choisir votre mot de passe car il sera nécessaire lors du déverrouillage de votre périphérique ou de la désinstallation d'ESET Mobile Security.

Sous l'onglet **Appliquer à**, vous pouvez spécifier les modules qui seront protégés par mot de passe.

Si vous oubliez votre mot de passe, vous pouvez envoyer un SMS à partir d'un numéro de téléphone enregistré dans votre liste **Amis de confiance** vers votre numéro de téléphone. Le SMS doit respecter le format suivant :
eset remote reset
Votre mot de passe sera réinitialisé.

9. Dépannage et assistance

9.1 Dépannage

ESET Mobile Security fournit une fonctionnalité de journalisation avancée qui facilite le diagnostic de problèmes techniques potentiels. Avant de contacter l'assistance à la clientèle d'ESET, il est recommandé de rechercher une solution possible dans la base de connaissances ESET. Si vous devez toujours contacter l'assistance à la clientèle d'ESET, suivez les étapes indiquées ci-dessous :

1. Allez à l'écran principal d'ESET Mobile Security, appuyez sur le bouton **MENU** puis sur **Paramètres de journalisation**.
2. Sélectionnez un composant du programme concerné par le problème.
3. Répliquez le problème. Des informations seront écrites dans un fichier journal de l'application.
4. Allez à l'écran principal d'ESET Mobile Security, appuyez sur le bouton **MENU** puis sur **Assistance à la clientèle**.
5. Si vous n'avez pas trouvé de solution dans notre base de connaissances, appuyez sur **Continuer**.
6. Inscrivez tous les détails et appuyez sur **Soumettre** au bas de l'écran de l'écran. Assurez-vous que l'option **Journal de l'application** est sélectionnée (par défaut).

9.2 Assistance technique

Nos spécialistes de l'assistance à la clientèle sont à votre disposition pour vous fournir de l'aide administrative ou de l'assistance technique relative à ESET Mobile Security ou à tout autre produit de sécurité d'ESET.

Pour trouver des réponses aux questions les plus fréquemment posées, consultez la base de connaissances ESET à l'adresse :
http://kb.eset.com/android

La base de connaissances contient une abondance d'informations utiles pour résoudre les problèmes les plus courants. Ces informations peuvent facilement être consultées par catégorie ou avec l'outil de recherche avancée.

Pour contacter l'assistance à la clientèle d'ESET, veuillez remplir le formulaire de demande d'assistance disponible à l'adresse :
http://eset.com/support/contact

Pour envoyer une demande d'assistance directement à partir de votre téléphone cellulaire, rendez-vous à l'écran principal d'ESET Mobile Security et appuyez sur le bouton **MENU**, suivi d'**Assistance à la clientèle**. Remplissez tous les champs requis. Pour inclure un **Journal de l'application** complet, suivez les étapes décrites dans la section Dépannage 11.